Open Redirect

- في موقع بيعمل Redirection لموقع تاني من غير ما يتاكد الموقع دا تابع للموقع ولا لا

```
https://example.com?redirect_uri=https://example2.com
uri=
url=
redirect=
```

- هنا بيعمل redirect من example.com لـ example2.com
- انت بتشيل الموقع التاني وتحط الموقع بتاعك لو وافق انو يعمل Redirect تبقي ثغره open Redirect
- اشهر ال Parameters ل open Redirect

- `?next={payload}`
- `?url={payload}`
- `?target={payload}`
- `?rurl={payload}`
- `?dest={payload}`
- `?destination={payload}`
- `?redir={payload}`
- `?redirect_uri={payload}`
- `?redirect_url={payload}`
- `?redirect={payload}`
- `/redirect/{payload}`
- `/cgi-bin/redirect.cgi?{payload}`
- `/out/{payload}`
- `/out?{payload}`
- `?view={payload}`
- `/login?to={payload}`
- `?image_url={payload}`
- `?go={payload}`
- `?return={payload}`
- `?returnTo={payload}`
- `?return_to={payload}`
- `?checkout_url={payload}`
- `?continue={payload}`
- `?return_path={payload}`

- لما بتلاقيهم بتجرب تغير ف الرابط التاني
- 

- الرابط التاني لازم يتعمل عليه encodeing لل (://) علشان السيرفر يفهم انهي الاول وانهي التاني
- لو ملقتش Parameters لل open Redirect بترح لاداة الـ arjun علشان تخمن ال Parameters
- ممكن بدل ما تغير الموقع تجرب فيه (javascript:confirm()) xss

---

- لو عملت Redirect ومنفعش كدا هتعمل bypass
- ممكن تشيل ال https اللي ف الموقع التاني وتخليه كدا //hacker.com
- https://hacktricks.boitatech.com.br/pentesting-web/open-redirect
- دا رابط موقع مجمع bypass كتير شوفهم
